Is Your Website Putting Your Design Firm at Risk?

A new wave of privacy lawsuit targets professional services websites.

Recently, there has been an increase in claims and litigation concerning website tracking and data collection practices. Primarily driven by heightened privacy awareness and evolving legal standards, professional service firm websites are being targeted for alleged violations of privacy and wiretapping statutes because of the use of tracking pixels, cookies, and similar technologies.

When a person visits a website, their activities typically are "tracked" by pixels, cookies and other similar technologies. That data often is then shared with third parties that use it for advertising and consumer identification. Sometimes this is referred to as "trap-and-trace" activity.

Courts have ruled that in certain contexts, state regulations regarding privacy protection, including wiretapping, prohibit this kind of activity. Design firms have been sued in states where they have no clients or projects on the theory that their website is accessible in that state. While this premise is currently under legal challenge, firms remain vulnerable, and some have chosen to settle out of court to avoid costly litigation and uncertain outcomes.

The California Consumer Privacy Act (CCPA), which came into effect in 2020, is one such statute that has significantly reshaped data privacy protections and drives much of this uptick in claims and litigation.[1] The CCPA grants California residents the right to know what personal information businesses collect, how it is used, and with whom it is shared. It also provides consumers the ability to opt out of the sale of their personal data and mandates businesses to implement transparent privacy notices. While the original intent of the legislation was to protect citizens from illegal wiretapping and eavesdropping activities, the scope of privacy litigation has been expanded to include tracking pixels and cookies, especially when used for targeted advertising or data sharing with third parties like Meta and Google.

The law emphasizes the importance of clear, accessible notices about data practices and informed consent, especially when it comes to tracking technologies like pixels and cookies. Companies must disclose whether they collect data through third-party trackers, such as advertising pixels, and clarify the purposes behind such data collection. Non-compliance can lead to enforcement actions, fines, and reputational damage.

---

[1] Other states' wiretapping statutes also are driving similar litigation. Plaintiffs are filing suits alleging violations of existing wiretapping statutes based on websites' unauthorized data collection via pixels and cookies. Some cases aim to challenge the legality of data sharing practices and the adequacy of cookie banners and disclosures.

A common thread in the trending claims and litigation is that website visitors were not notified upfront that (i) their use of the website is being tracked and (ii) the resulting data is being shared with third parties. Firm leaders may not be aware that their firm's website is tied to a third-party entity such as LinkedIn or Meta. To avoid being the target, design firms are advised to:

- examine their website tracking mechanisms to determine what, if any, data collection and/or tracking is taking place and whether it is provided to third parties,
- evaluate compliance with privacy laws, and
- provide transparent disclosures to users as needed to mitigate legal risks.

This proactive approach may include making sure your firm's website provides a notice allowing visitors to opt out of the sharing of information for analytics purposes and requiring the user to consent before they can go any further on the site.

Shehla Qureshi, AXA XL Cyber Claims Manager, emphasizes the importance of transparency: "Being aware of what you're tracking, why you're doing it, and informing users accordingly so that informed consent is truly in place is critical in mitigating legal risks associated with pixel tracking."

To protect your firm, we recommend the following action items:

1. Be aware the tracking capabilities of your firm's website
2. Implement and display an easily understandable cookie banner that requires the user to affirmatively consent to data collection
3. Limit website tracking to narrow, justified purposes
4. Monitor related statutory and legal developments

Taking these steps helps your organization demonstrate a commitment to privacy compliance, reduce the risk of litigation, and promote transparency with your users. Should you receive notice of a lawsuit or potential lawsuit related to website activity tracking, notify your broker immediately.